



YOU DESERVE THE BEST SECURITY

CASE STUDY

**PHOENIX PETROLEUM PARTNERS WITH
CHECK POINT TO EFFICIENTLY MANAGE
AND MITIGATE EXTERNAL CYBER RISKS.**

Introduction

Phoenix Petroleum deployed Infinity ERM to continuously monitor all its digital assets—from domains and IP addresses to brand names and the names of executive leaders. By quickly identifying relevant threats, Infinity ERM helps Phoenix Petroleum to take action and mitigate risks before they evolve into serious security incidents.

Challenge: Continuously Monitoring An Array Of Digital Assets & Proactively Managing External Cyber Risks

Phoenix Petroleum started as a family business in 2002 in the southern Philippines and has since grown into a thriving nationwide network of retail and commercial channels, with a diverse product line that services both individual and industrial clients.

Phoenix Petroleum's rapid rise as a key oil company in the Philippines led to a much greater number of digital assets, a larger attack surface, and an increased level of cyber risk to manage.

The challenge is that the attack surface is constantly evolving, and so is the threat landscape. New digital assets are created and deployed and new CVEs are discovered in up-to-date software. Meanwhile, threat actors develop new TTPs and launch new attack campaigns. Staying ahead of all these risks is a difficult project that requires continuous vigilance, cyber expertise, mature processes, and innovative technologies.

Challenges

- Gaining visibility across the web to continuously monitor digital assets
- Detecting impersonation attacks on phishing sites & fraudulent social profiles
- Managing a large external attack surface and rapidly identifying vulnerabilities

Solution

- Deployed the Check Point Infinity ERM solution

Impact

- Increased visibility and continuous monitoring of all digital assets
- Deep & dark web monitoring with real-time alerting on relevant threats
- A proactive approach to identifying and mitigating external cyber risks

"We looked at some other vendors and they have good solutions, but we needed more than what they could offer. With Infinity ERM, I can continuously monitor not only all of Phoenix Petroleum's domains, but all our digital assets, plus we get relevant intelligence from the deep and dark web."

Roland Villavieja, Information Security Officer at Phoenix Petroleum

Visibility On Impersonation Attempts & Fraudulent Activity Across The Web

Like all large enterprises, Phoenix Petroleum is sometimes impersonated by cyber criminals who seek to profit from illegal scams. These attacks include everything from lookalike domains and phishing sites that mimic Phoenix Petroleum's legitimate website to fraudulent social media profiles that masquerade as an official account or as members of the executive leadership team.

"Infinity ERM was able to detect impersonation on social media of members of our senior management team – and they were very surprised to see these fraudulent profiles," said Roland Villavieja, Information Security Officer at Phoenix Petroleum. "It's very difficult to identify fraudulent social media profiles like those unless you have a solution like Infinity ERM."

Continuous External Asset Discovery & Real-Time Vulnerability Detection

As a major energy producer, Phoenix Petroleum has many domains and IP addresses to monitor and manage. With the attack surface constantly shifting—new assets being deployed, new software and services getting installed on existing assets, and new risks coming to light—an automated solution is essential.

With Infinity ERM, Phoenix Petroleum can continuously map out the attack surface, check assets for potential issues, and receive real-time alerts for major risks that require immediate action. Infinity ERM creates a full inventory of both assets and the technologies visible in the external attack surface. Risk severity levels are assigned to each asset for simplified prioritization and remediation.

" One of the things I like is that Infinity ERM checks whether my external assets are vulnerable from an attacker's point of view. So, for example, when a new CVE is discovered, I know immediately if I have that vulnerability in my attack surface and I can access threat intelligence on that CVE."

Easy & Efficient External Cyber Risk Management

The cybersecurity team at Phoenix Petroleum is managing several priorities: standing up new cyber technologies, achieving compliance with major frameworks, and staying ahead of an increasingly hostile threat landscape.

Check Point recognizes that many cybersecurity teams are short on time and resources, but long on tasks and projects. To help cyber teams better manage the workload and reduce risk, the Infinity ERM solution was designed for efficiency.

"Infinity ERM gives me confidence and helps me sleep easy at night because I know someone is constantly monitoring our digital assets. This frees up my time to focus on other priorities," said Phoenix Petroleum's Information Security Officer Roland Villavieja.

Worldwide Headquarters

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters

100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com