

Phoenix Energy Marketing Consultants, Inc.



Location

Calgary, Canada

Industry

Energy

The Need

- An extra layer of protection to supplement the existing spam and anti-virus filters.
- An automated solution to replace the manual process of implementing individual block lists.
- To comply with Canada's (PIPEDA) and Alberta's (PIPA) information security laws.

The Solution

- ThreatSTOP automates the aggregation, correlation, updating, delivery and enforcement of real-time IP reputation intelligence to customers.
- Saves time and eliminates drudgery of manual process.
- Provides peace of mind and extra insurance against data loss.

Customer Overview

Phoenix Energy Marketing Consultants is an independent energy marketing and consulting firm for the Western Canadian oil & gas industry. Phoenix Energy currently serves over 40 producer clients representing approximately 20,000 barrels a day of crude oil, 4,000 bbls/day of NGL's and 120 million cubic feet per day of natural gas production. Its training division provides introductory courses in crude oil, natural gas and NGL marketing that are recognized as industry benchmarks.

Phoenix Energy's IT systems consist of a Microsoft backend, Juniper firewall, VPN for its remote consultants, Symantec Enterprise Security, and a MX Logic (McAfee) spam filter in an edge proxy for e-mail.



The Need

For a small company with one location and remote contractors coming in through VPN, Phoenix Energy was reasonably protected, and it had not experienced any major breaches in recent years. But Carol Maffitt, Phoenix Energy's CIO, wanted an extra layer of protection, for added peace of mind. "I don't relish the idea of a security breach and data loss," explained Carol. "I want to make sure we are as protected as possible and that we comply with the information security regulations." In Phoenix Energy's case, it has to comply with both the federal Canadian law (PIPEDA) and Alberta Province's PIPA.

Previously, Carol had been downloading various block lists, and manually updating, aggregating and inputting them into the Juniper firewall. She then had to parse the firewall logs to try to find problems quickly, which was difficult to do. The whole process was tedious and time-consuming.

The Solution

Looking for a better solution, Carol found ThreatSTOP through a link on DShield.org and immediately saw the benefits of ThreatSTOP, namely:

- Aggregating many threat feeds into one actionable block list
- Continuous updates of the block list
- Automating the delivery of the block list into the firewall for enforcement

Additionally, ThreatSTOP provides clear Web-based reports to:

- Summarize attempted breaches so the hosts in question can be investigated or remediated
- Profile each bad IP address to support forensic investigation and/or prosecution

These reports are much easier to digest than firewall log files, and they are included in the ThreatSTOP service.

With ThreatSTOP, Phoenix Energy's IT group now spends much less time doing the drudge work of protecting the company and more time on higher-value activities. "Now I look at the ThreatSTOP reports about twice a week just to make sure everything is working and no major problems have occurred," Carol concluded.

"By automating the process and providing the reports, ThreatSTOP provides me a peace of mind and saves me time."

Carol Maffitt

CIO

Phoenix Energy Marketing Consultants