FORCEPOINT

Enterprise Oil & Gas Company

Within mere weeks, the product's pilot deployment surfaced not one but two separate cases of access abuse by privileged users—employees exfiltrating sensitive data.

Industry
Energy, Oil & Gas

Country
United States

Issue
Securing critical data from people-based vulnerabilities

Product
Forcepoint Insider Threat

Overview

A Fortune US 100 & Fortune Global 500 Energy company is engaged in every aspect of the oil, natural gas, and geothermal energy industries. These include hydrocarbon exploration and production, refining, marketing and transport, chemicals manufacturing and sales, and power generation. The company manufactures and sells products such as fuels, lubricants, additives, and petrochemicals, with alternative energy operations including geothermal, solar, wind power, biofuel, fuel cells, and hydrogen.

Challange

The company stores a variety of valuable data: internal patents, intellectual property (IP), merger and acquisition data, machine schematics, and geological data like potential drill sites. Many of those with access to this sensitive data are temporary contractors, employed for only a brief period of time. Understanding the higher risk that accompanies shorter-term employees, company leaders brought in third-party analysts to do an assessment of insider threat risk.

Analysts found that data was indeed leaving the company, and that nearly half of the data loss incidents were directly related to the actions of negligent or malicious insiders. Upon hearing the results, company leaders authorized the creation of an internal insider threat task force; much of this team had direct experience working with the federal government and were familiar with Forcepoint Insider Threat, a sixteen-year-old product incepted at the R&D departments at Raytheon. Thus, a pilot deployment began with 1,100 licenses, during which the product underwent a rigorous testing period.

Get in touch with us.

Learn how Forcepoint can protect you. Contact us at **forcepoint.com/contact**.

Detailed incident reporting and DVR functionality provide context around potential data loss incidents, the most recent of which had involved an employee stockpiling sensitive data to take to a competitor.

Solution

It didn't take long for Forcepoint Insider Threat to make an impact. Within mere weeks, the product's pilot deployment surfaced not one but two separate cases of access abuse by privileged users—employees exfiltrating sensitive data. While the pilot program had garnered executive visibility, these discoveries in particular hastened the management team's buy-in.

The Forcepoint team spent several months working closely with the company's leaders to understand their desired business and security outcomes. In addition to the initial product onboarding, countless hours were spent conveying the corporate vision, Forcepoint's human-centric cybersecurity strategy, and product roadmap. The management team appreciated how Forcepoint Insider Threat could integrate with other Forcepoint—as well as third-party—solutions to provide a more comprehensive overall security posture. Offered a flexible deployment and license structure that aligned with its budgetary objectives, the company moved forward with the purchase of 80,000 seats of Forcepoint Insider Threat.

Results

Looking back on the product's first months of use, the company's leaders offered glowing reviews, calling it "a reliable product that gives in-depth visibility into risky user activity, especially at the endpoint level." Detailed incident reporting and DVR functionality provide context around potential data loss incidents, the most recent of which had involved an employee, new to the organization from a recent merger. The employee began stockpiling sensitive data to take to a competitor, concerned they would be terminated after the acquisition.

Speaking on the incident, one team member had the following to say: "The product's DVR playback functionality provided helpful forensics and investigation, a tremendous help when monitoring for potentially malicious end-user activity. The discovery of the recent data stockpiling prevented a major data loss incident and thousands of dollars in IP loss. Most importantly, it helped us avoid a scathing front-page headline and the possible loss of long-standing accounts."

Forcepoint's rich experience in the insider threat space assures the company's management they have chosen the right vendor to protect their critical data. Shortly after the deployment, the company purchased an undisclosed number of data loss prevention (DLP) and user and entity behavior analytics (UEBA) seats. This pairing has opened the door to risk-adaptive protection, a proactive security approach that integrates behavior analytics and enforcement to quickly identify high-risk activity and automate the response according to real-time changes in risk.

According to company leaders, "Forcepoint Insider Threat is the most mature, scalable and feature rich insider threat solution in the market today. Couple that with how they challenged our technical team to think differently, this decision was a no-brainer."