Forcepoint

Customer Story

Data is the New Oil, and This Enterprise Keeps its Competitive Edge by Protecting Both with Forcepoint

A multinational oil and gas company attunes to its people to build a safer environment for proprietary data.

Improving safeguards around proprietary data even as employees come and go cultivates a safer environment to advance the overall mission of this large energy enterprise. They needed a way to see just how their 50,000+ employees were interacting with sensitive company assets. A Forcepoint consulting engineer explained, "They knew there were leaks, but they weren't able to get ahead of them." With Forcepoint Insider Threat, the organization has not only the deeper visibility they need, but also the rich forensics to support conclusive investigations.

CUSTOMER PROFILE:
This Fortune U.S. 50 enterprise oil and gas company is engaged in the industry at every level from production to retail.

INDUSTRY:
Oil and gas

HQ COUNTRY:
United States

PRODUCT:
Forcepoint Insider Threat

50% of data leakage was an inside job

There are few more challenging environments than one that supports the production and distribution of one of the world's most valuable and limited resources. As an organization deeply engaged in every aspect of oil, natural gas, and geothermal energy, the amount of critical proprietary data this company relies on is staggering.

While the most common data breaches can mean leakage of customer and consumer data leading to a reputational hit, a leak of this enterprise's most critical information, including invaluable geographical data and retail market pricing strategies, could directly undermine its competitive position, revenue, and market share for years to come.

So, when a third-party analyst confirmed that half of the company's data leakage resulted from its own workforce, the company put together a task force to identify a security solution specifically tailored to guard against inside threats.

A tightly knit industry brings complex challenges in safeguarding valuable resources

The task force started by identifying the company's biggest risk: employees leaving the company—whether they resign, are let go, or are ending a contract.

"The oil and gas industry is actually a pretty small community, so it's very likely that employees would go to a competitor organization if they leave," explained Forcepoint consulting engineer Romares Barnett. "The client wanted to be aware of who their risky users were so they could work to prevent potential issues—before the data was taken and handed to a rival."

The company would become aware after an employee had exfiltrated proprietary information, but had no ability to understand if it was an accident or prove that data theft had happened maliciously. In the worst-case scenario, the enterprise wanted to ensure it could take appropriate action by having the ability to prove the action was intentional.

The task force identified the need for a security solution that could provide better monitoring of its users' behavior, more effective indicators of potential threats, and improved documentation. Several members had direct experience working within the federal government and were familiar with Forcepoint Insider Threat (IT), a proven solution generated by the R&D department of defense contractor Raytheon. That made it an easy decision to tap Forcepoint for an initial pilot program, focused on monitoring 1,000 users with access to the organization's most sensitive information.

> "The client wanted to be aware of who their risky users were so they could work to prevent potential issues—before the data was taken and handed to a rival."
>
> **ROMARES BARNETT,** CONSULTING ENGINEER, FORCEPOINT

Saving thousands of dollars with a closer view into data movement

IT provides complete visibility into user behavior at the endpoint, including monitoring of communications channels, to help identify potential flight risks or disgruntled workers. It also provides visibility into user attempts to change file names, screen-capture sensitive documents, and attempt system process changes while offline.

The solution also met the organization's investigative needs with detailed forensics like timelines, live video capture, and replay of individual user actions. Compared to competitors, Forcepoint's video capabilities capture a longer time frame and provide full-color video playback.

Challenges

Secure critical proprietary data from people-based vulnerabilities.

Optimize and enhance investigations of data loss and theft incidents.

Approach

Deploy Forcepoint Insider Threat to gain visibility into employee interactions with sensitive data and provide detailed reporting and video playback to capture context and intent.

Within mere weeks, the IT pilot surfaced three separate cases of access abuse by privileged users—employees exfiltrating sensitive data—which the solution helped to curtail. The most recent example involved a new employee from a recent merger. Concerned about being terminated after the acquisition, the employee began stockpiling sensitive data to take to a competitor. The discovery of the data stockpiling prevented a major data loss incident and hundreds of thousands of dollars in IP loss.

From the pilot program the task force extrapolated the impact that IT could have across the company: three incidents among a thousand-user pilot opened their eyes to what they could be missing within their 50,000-plus user workforce. "They really wanted to know what they weren't seeing," said Barnett.

Context provides irrefutable evidence to speed time to resolution

Since rolling out IT worldwide, the security staff have optimized investigation time by prioritizing threats through deep forensics around events. The organization can more quickly review incidents and determine which are truly concerning.

IT's video recording also provides the enterprise with irrefutable evidence when there is malicious intent, saving money in potential litigation. "They're able to determine if a person is just looking to post a job for the company, or if they're filling out an application to work at a competitor," explained Barnett. "By recording 10 minutes before the triggered incident and 10 minutes after, they have the context they didn't have before."

2

cases of insider data exfiltration within weeks of pilot deployment

1

data stockpiling incident discovered in time to prevent major loss

> "By recording 10 minutes before the triggered incident and 10 minutes after, they have the context they didn't have before."

ROMARES BARNETT, CONSULTING ENGINEER, FORCEPOINT

As the organization worked more closely with Forcepoint as a trusted partner, they shifted toward a more humanly attuned approach to workforce protection—and to cybersecurity in general. Freed from the overwhelming incident-by-incident security, the security team can now employ risk-based analysis to prioritize effort where it will be most valuable.

Always seeking to create new value, the organization is undertaking a proof of concept for Forcepoint Data Loss Prevention and Behavioral Analytics. This pairing opens the door to risk-adaptive protection, a security approach that integrates analytics and enforcement to quickly identify high-risk activity and automatically tune the security 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 the fact Forcepoint is flexible and challenged our technical team to think differently, we're convinced we chose the best partner."

Results

2 detected cases of insider data exfiltration within weeks of pilot deployment.

1 data stockpiling incident discovered in time to prevent major loss of IP, money, and reputation.

Reduced time to investigation resolution.

Increased ability to provide irrefutable evidence in the case of litigation.

> "We're convinced we chose the best partner."

COMPANY LEADER, OIL AND GAS COMPANY