



# Data Mining: Ransom Payment Advisory

## Case Background

Our client, a global leader in engineering with offices in six continents, experienced a ransomware incident. A forensic investigation determined that protected health information (PHI), intellectual property (IP), and personal identifiable information (PII) was potentially exfiltrated from the environment. Although our client had viable backups, analysis was still needed to determine if the risk of data leakage from the extortion threat was significant enough to warrant a ransom payment.

## Business Challenge

The client looked to use data mining outputs to drive their business decision on a ransom payment against the threat actor's seven-day clock. Additionally, the client had systems spread across the globe and faced strict GDPR reporting deadlines. During the initial review, the team identified over 20 systems containing a total of 1.5 TB of data that required analysis. A manual review of this data would have taken approximately three months.

## Unique Approach

Leveraging unique technology, MOXFIVE quickly built a plan to assess over 870,000 files and determine if they contained PHI, IP, and PII. The agentless approach allowed us to start processing the data within 24 hours. Using both out-of-the-box and custom rulesets, combined with proprietary machine learning techniques, we were able to complete the project in approximately seven percent of the time that a manual review would have taken.

## Conclusion

Executing this approach, we were able to help our client determine that the data set did not contain significant sensitive information that would put client or employees at risk and that the data exfiltration did not contain intellectual property that would jeopardize the business if leaked. With this information, our client was able to decide that paying the ransom was not necessary.

## RESULTS



**Reduced overall timeline from 3 months to 1 month**



**Deployed and mining data within 24 hours**



**Processed 1.5 TB in one week**



**Avoided ransom payment**



**Increased confidence in results**




**Certified report that is easily digestible**

## OTHER USE CASES

- Intellectual Property
- Mergers & Acquisitions
- Complex Legal Matters

MOXFIVE is a cybersecurity company helping organizations respond to incidents and minimize the risk of future attacks. Over the last decade, our team of experts has helped thousands of businesses respond to major incidents and saw firsthand that there needed to be a better way for organizations to get the technical expertise they need when they need it most. Through a combination of our technical experts and proprietary platform, we bring order to chaos and deliver a tailored incident response approach and resilience-minded path forward for clients of all sizes, faster and more efficiently.

 [www.moxfive.com](http://www.moxfive.com)

 (833) 568-6695

 [info@moxfive.com](mailto:info@moxfive.com)