proofpoint. | **CITIC PACIFIC MINING**

CITIC Pacific Mining protects people and sensitive data with Proofpoint

Challenge

- Secure mining organization against escalating email threats
- Keep company leadership informed about security posture
- Keep mining operations running smoothly and reliably

Solution

- Proofpoint Threat Protection (Email Security)
- Proofpoint Information Protection
  - Proofpoint Endpoint Data Loss Prevention
  - Proofpoint Cloud App Security Broker
  - Proofpoint SaaS Isolation
  - Proofpoint Insider Threat Management
- Proofpoint Email DLP and Encryption
- Proofpoint Intelligent Classification and Protection
- Proofpoint ZenGuide™ (formerly Proofpoint Security Awareness
- Proofpoint Email Fraud Defense

Results

- Proofpoint Information Protection Suite provides user behavior context to strengthen security practices
- Quarterly business reviews provide security posture and investment insights

The organization

CITIC Pacific Mining (CPM), a wholly owned subsidiary of Hong Kong's CITIC Limited, relies on data for insights about its operations and efficiency. Headquartered in Perth, the company was established to manage the construction and operation of Sino Iron, an integrated mining, processing and port operation supplying high-grade, low impurity iron ore product to the steel mills of Asia.

The challenge

Keeping mining operations and processes secure

Nonstop innovation is a core value at CPM. The organization is constantly striving to maximize its production levels and optimize mining, processing, product loading and other systems. The network infrastructure is fundamental to the company's mission, and keeping it safe and secure is top of mind. Protecting the integrity of email communications is a top priority. But the company's previous email security solution was unable to keep pace with the latest threats.

"When I first started working here, I was seeing 10 unwanted emails in my inbox a day, and for some of the existing employees, I expect the number was 10 times higher," said Spencer Lai, Principal Information Security & Risk at CITIC Pacific Mining. "We needed to move to something more secure, because the nature of our industry makes us quite vulnerable to any cybersecurity attack."

Spencer and his team did their due diligence. They worked in partnership with Lumen IT, a local provider of cybersecurity solutions to evaluate email protection products from a variety of vendors. After exploring their options, the team found that

Proofpoint Email Protection provided the strongest set of features, and was highly regarded by industry experts.

"We evaluated several solutions, but they weren't meeting our requirements," said Spencer. "We were seeking a solution that was more cloud-based. We looked at Gartner Magic Quadrant reports, and read lots of good things about Proofpoint, so we chose their solution. Proofpoint has resolved our issue of receiving malicious and unwanted emails."

The solution

Building data context and insights

After years of using Proofpoint Email Protection, CPM has been pleased with its ability to stop email fraud, phishing, viruses and more. Perhaps just as important, the solution gives Spencer and his team visibility and a deeper understanding of the company's security posture. And it helps the company's business leaders understand the business outcomes that their investment delivers.

"It's good to know what the platform is seeing in a simple dashboard, and it also helps me communicate this to our leadership," said Spencer. "Business leaders are always looking for cost justification, and the quarterly business reviews help tell the whole story. This improves buy-in from our stakeholders."

Now Spencer and his team have launched an initiative to extend the capabilities of their solution. Lumen IT had played a key role in the deployment of Proofpoint Email Protection, and is working closely with CPM to expand the solution to support the organization's data loss prevention (DLP) initiatives.

"Our Proofpoint quarterly business review is really valuable to us. And not just for email security, but cybersecurity solutions as a whole."

SPENCER LAI,
PRINCIPAL INFORMATION
SECURITY & RISK,
CITIC PACIFIC MINING
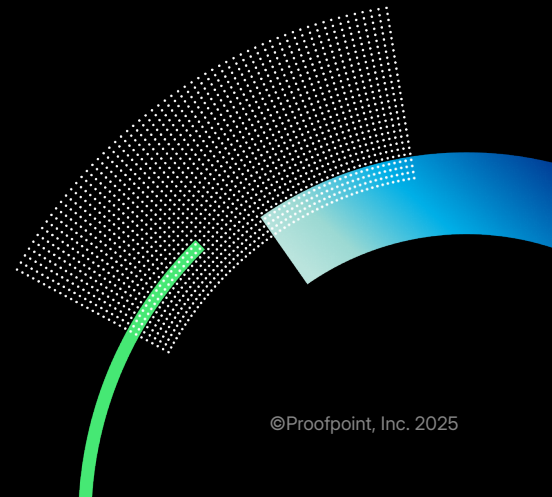
"We have progressively evolved to use more and more Proofpoint solutions," said Spencer. "We're currently on a journey to make full use of data loss prevention, because of the confidence we have with regards to Proofpoint."

Lumen IT recommended a suite of solutions, including Proofpoint DLP Transform (a bundle of Cloud App Security Broker, Endpoint DLP and Insider Threat Management) and Proofpoint Intelligent Classification and Protection.

Proofpoint DLP Transform accurately identifies sensitive content and provides deep visibility into user behavior. With this solution, CPM can quickly detect impactful data loss risk across cloud and endpoints and take appropriate action.

"When we started considering the use case for data loss prevention, we realized that extending Proofpoint makes sense," said Spencer. "You can start off looking at email security, but then realize that Proofpoint has visibility of data that goes through the gateway."

A brief POC with Lumen IT had found significant risk around cloud-based application use. This included multiple illegal login attempts from overseas locations and access to unsanctioned applications. Lumen IT recommended Proofpoint Cloud App Security Broker (CASB) to help the organization secure its cloud users, apps and data from threats, data loss and compliance risks.

The results

Toward a human-centric approach to cybersecurity

Spencer and his team expect that the enhanced Proofpoint solution will provide capabilities that the organization's current endpoint detection and response (EDR) system can't offer.

"With the DLP Transform solution in place, Proofpoint should be able to better inform us in terms of the sensitivity of data," he said. "Our EDR product might tell us that we have seen large data movement by certain users. But our EDR is not a DLP solution, and it doesn't have the capability to examine data and determine whether it is sensitive. For example, in our industry, users will sometimes need to take footage of what's actually happening at a site and share large video files with a vendor or a third-party cloud. But large data volume is not always an indicator of risk. DLP gives us the context we need to understand more."

With Proofpoint DLP Transform, CPM is not only gaining a better understanding of how users are working with data, but also acquiring the information it needs to build a stronger company culture of security.

"Proofpoint calls it a human-centric approach, and it's true," said Spencer. "It's more than just receiving an alert from our EDR system based on endpoint or device. Proofpoint gives us more context into user behavior, and where the person is trying to log on from. So having a conversation with the end user if we suspect an incident is much easier, because we have all the facts and contacts, and can confirm with them what has actually happened."

Proofpoint CASB provided immediate benefits in terms of identifying cloud application risk. The solution has given CPM the ability to protect sensitive data and respond to cloud security incidents with instant context.

To further enhance its protection, CPM is also deploying Proofpoint Intelligent Classification and Protection. This advanced solution uses an AI model to analyze and classify data, and recommends how best to prioritize the protection of the company's most sensitive data—not only for current employees, but past ones.

"Like many organizations, we also have the usual cases of resigned users who move data around, and I'm sure that's quite common," said Spencer. "Therefore, we needed that kind of visibility, so that's a picture these solutions will be able to piece together for us."

With its robust email security and intelligent DLP capabilities, CPM can rest assured that it is keeping data and mining operations safe and secure across the extended enterprise.

proofpoint.

DISCOVER THE PROOFPOINT PLATFORM →