

## KUNDENBERICHT

# CITIC Pacific Mining schützt Mitarbeiter und vertrauliche Daten mit Proofpoint

### Herausforderung

- Schutz des Bergbauunternehmens vor stark zunehmenden E-Mail-Bedrohungen
- Kontinuierliche Information der Unternehmensleitung über aktuelle Sicherheitslage
- Gewährleistung des reibungslosen und zuverlässigen Bergbaubetriebs

### Lösung

- Proofpoint Threat Protection (E-Mail-Sicherheit)
- 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™ (ehemals Proofpoint Security Awareness)
- Proofpoint Email Fraud Defense

### Ergebnisse

- Die Proofpoint Information Protection-Suite liefert Kontext zum Anwenderverhalten, um Sicherheitsmaßnahmen zu unterstützen
- Vierteljährliche Business Reviews liefern Einblicke zur Sicherheitslage und zu Investitionen

### Das Unternehmen

CITIC Pacific Mining (CPM), eine hundertprozentige Tochtergesellschaft von CITIC Limited in Hongkong, benötigt Daten für Einblicke zu den eigenen Abläufen und deren Effizienz. Das Unternehmen mit Hauptsitz in Perth (Australien) verwaltet den Bau und Betrieb von Sino Iron, einem integrierten Bergbau-, Verarbeitungs- und Hafenunternehmen, das hochgradiges Eisenerz mit geringen Verunreinigungen an die Stahlwerke in Asien liefert.

### Die Herausforderung

#### Gewährleistung der Sicherheit des Bergbaubetriebs und seiner Prozesse

Ständige Innovation ist einer der zentralen Werte von CPM. Das Unternehmen ist stets bestrebt, seine Produktion zu steigern und den Abbau, die Verarbeitung und die Verladung der Produkte sowie andere Systeme zu optimieren. Für die Mission des Unternehmens ist die Netzwerkinfrastruktur von grundlegender Bedeutung. Ihre Sicherheit hat daher besonders wichtig. Höchste Priorität hat dabei die Integrität der E-Mail-Kommunikation. Hier konnte die bisherige E-Mail-Sicherheitslösung des Unternehmens mit den neuesten Bedrohungen nicht mehr Schritt halten.

„In meiner Anfangszeit bei CPM fand ich jeden Tag 10 unerwünschte E-Mails in meinem Posteingang. Bei einigen Kollegen waren es eher noch zehnmal mehr“, berichtet Spencer Lai, Principal Information Security & Risk bei CITIC Pacific Mining. „Da unsere Branche für Cyberangriffe ziemlich anfällig ist, mussten wir auf eine sicherere Lösung umsteigen.“

Lai und sein Team sind bei der Anwendersuche sehr sorgfältig vorgegangen. In Zusammenarbeit mit Lumen IT, einem lokalen Anbieter von Cybersicherheitslösungen, prüfte das Team von CPM die E-Mail-Sicherheitsprodukte verschiedener Anbieter und entschied sich letztendlich für Proofpoint Email Protection, weil die Lösung den besten Funktionsumfang bietet und von Branchenexperten hoch geschätzt wird.

„Wir haben mehrere Lösungen evaluiert, aber sie entsprachen nicht unseren Anforderungen“, erklärt Lai. „Wir suchten eine Cloud-basierte Lösung und haben in den Gartner Magic Quadrant-Berichten viel Gutes über Proofpoint gelesen. Deshalb haben wir uns für ihre Lösung entschieden. Proofpoint hat unser Problem der schädlichen und unerwünschten E-Mails im Posteingang aus der Welt geschafft.“



## Die Lösung

### Datenkontext und Einblicke

Nach mehreren Jahren mit Proofpoint Email Protection ist das Unternehmen sehr angetan davon, wie die Lösung E-Mail-Betrug, Phishing, Viren und mehr stoppt. Ein vielleicht ebenso wichtiger Aspekt ist jedoch auch, dass die Lösung Lai und seinem Team mehr Transparenz bietet und ein besseres Verständnis von der Sicherheitslage des Unternehmens ermöglicht. Zudem hilft sie der Geschäftsleitung des Unternehmens, die geschäftlichen Vorteile ihrer Investition zu erkennen.

„Es ist sehr hilfreich, alle Informationen der Plattform in einem einfachen Dashboard anzeigen zu können. Das vereinfacht auch die Kommunikation mit unserer Geschäftsleitung“, sagt Lai.

**„Die vierteljährlichen Business Reviews von Proofpoint sind für uns sehr wertvoll – nicht nur in Bezug auf die E-Mail-Sicherheit, sondern auch für die Cybersicherheitslösungen insgesamt.“**

**SPENCER LAI,  
PRINCIPAL INFORMATION  
SECURITY & RISK,  
CITIC PACIFIC MINING**



„Führungskräfte legen großen Wert darauf, dass Kosten auch begründet werden, und die vierteljährlichen Business Reviews helfen bei der Vervollständigung des Gesamtbilds. Dadurch steigt die Akzeptanz bei unseren Stakeholdern.“

Inzwischen haben Lai und sein Team eine Initiative gestartet, um die Möglichkeiten ihrer Lösung weiter auszubauen. Lumen IT spielte bei der Einführung von Proofpoint Email Protection eine Schlüsselrolle und arbeitet nun eng mit CPM zusammen, um die Lösung so zu erweitern, dass sie das Unternehmen auch bei der Datenverlustprävention (DLP) unterstützt.

„Wir haben nach und nach immer mehr Proofpoint-Lösungen eingeführt“, erklärt Lai. „Momentan arbeiten wir daran, alle DLP-Funktionen für uns zu erschließen, weil wir Proofpoint vertrauen.“

Lumen IT empfahl unter anderem die Lösungssuites Proofpoint DLP Transform (ein Paket aus Proofpoint Cloud App Security Broker, Proofpoint Endpoint DLP und Proofpoint Insider Threat Management) und Proofpoint Intelligent Classification and Protection.

Proofpoint DLP Transform kann vertrauliche Inhalte zuverlässig identifizieren und bietet umfassende Einblicke in das Anwenderverhalten. Mit dieser Lösung kann CPM Datenverlustrisiken in der Cloud und auf Endpunkten schnell erkennen und entsprechende Maßnahmen ergreifen.

„Bei den ersten Überlegungen zum Use Case für DLP wurde uns schnell klar, dass eine Erweiterung unseres Proofpoint-Portfolios sinnvoll ist“, berichtet Lai.

„Wir hatten zunächst nur die E-Mail-Sicherheit im Blick, erkannten dann aber, dass Proofpoint Informationen zu den Daten hat, die das Gateway passieren.“

In einem kurzen Proof of Concept mit Lumen IT wurden erhebliche Risiken durch die Nutzung von Cloud-Anwendungen erkannt, darunter mehrere illegale Anmeldeversuche von ausländischen Standorten sowie Zugriffe auf nicht genehmigte Anwendungen. Lumen IT empfahl Proofpoint Cloud App Security Broker (CASB) zum Schutz der Cloud-Nutzer, -Anwendungen und -Daten vor Bedrohungen, Datenverlust und Compliance-Risiken.

## Die Ergebnisse

### Wechsel zu einem personen-zentrierten Cybersicherheitsansatz

Lai und sein Team erwarten, dass die erweiterte Proofpoint-Lösung Möglichkeiten bietet, mit denen das aktuelle EDR-System (Endpoint Detection and Response) des Unternehmens nicht mithalten kann.

„Nach dem Hinzufügen von Proofpoint DLP Transform sollten wir noch bessere Aussagen zur Vertraulichkeit von Daten erhalten“, sagt er. „Unser EDR-Produkt kann uns vielleicht informieren, wenn bestimmte Anwender große Datenmengen bewegen. Es ist jedoch keine DLP-Lösung, die Daten untersuchen und dann sagen kann, ob diese vertraulich sind. In unserer Branche müssen die Anwender zum Beispiel gelegentlich Aufnahmen von aktuellen Geschehnissen an einem Standort machen und große Videodateien an eine Anbieter senden oder in eine Drittanbieter-Cloud hochladen.“

Große Datenvolumen sind daher nicht immer ein Risikoindikator. Dank DLP steht uns der erforderliche Kontext für ein besseres Verständnis zur Verfügung.“

Mit Proofpoint DLP Transform versteht CPM nicht nur besser, wie Anwender mit Daten umgehen, sondern erhält auch die Informationen, die für den Aufbau einer stärkeren Sicherheitskultur im Unternehmen benötigt werden.

„Proofpoint spricht von einem personenzentrierten Ansatz und das stimmt auch“, so Lai. „Es geht um mehr als endpunkt- oder gerätebezogene Warnungen vom EDR-System. Proofpoint liefert uns Kontext zum Anwenderverhalten und zu dem Standort, von dem aus eine Person versucht sich anzumelden. Dann können wir im Verdachtsfall viel einfacher mit dem Endnutzer sprechen, weil wir alle Fakten und Kontakte haben und mit ihm klären können, was wirklich passiert ist.“

Proofpoint CASB bot bei der Identifizierung von Risiken durch Cloud-Anwendungen unmittelbare Vorteile. Die Lösung lieferte CPM sofort Kontext, sodass sie

vertrauliche Daten schützen und auf Cloud-Sicherheitszwischenfälle reagieren können.

Um den Schutz weiter zu verbessern, implementiert CPM auch Proofpoint Intelligent Classification and Protection. Diese hochentwickelte Lösung nutzt ein KI-Modell für die Analyse und Klassifizierung von Daten und gibt Empfehlungen, wie der Schutz der vertraulichsten Daten des Unternehmens am besten priorisiert werden kann – nicht nur für aktuelle, sondern auch für ehemalige Mitarbeiter.

„Wie in vielen Unternehmen gibt es auch bei uns Fälle von ausgeschiedenen Anwendern, die Daten noch irgendwie verschieben. Ich bin sicher, dass das ziemlich oft vorkommt“, meint Lai. „Wir benötigten hierfür genau diese Transparenz – und wir werden sie mit diesen Lösungen erhalten.“

Dank der zuverlässigen E-Mail-Sicherheit und der intelligenten DLP-Funktionen kann CPM darauf vertrauen, dass die Daten und der Bergbaubetrieb im gesamten Unternehmen geschützt sind.

# proofpoint®

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 85 Prozent der Fortune 100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter [www.proofpoint.de](http://www.proofpoint.de).

Verbinden Sie sich mit Proofpoint: [LinkedIn](#)

Proofpoint ist eine eingetragene Marke von Proofpoint, Inc. in den USA und/oder anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.

**LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN** →