voices

CrowdStrike Customer Case Study

CrowdStrike Reinforces Safety for Staff at One of the World’s Leading Mining and Infrastructure Solutions Providers

Deep in the heart of the Australian outback, an explosives expert waits for a laptop to record data from a blast in a mine shaft hundreds of feet underground. Around the world, in remote environments, thousands of laptop, device and system endpoints are used by Orica mining personnel to help customers improve the discovery and extraction of essential raw materials. It is the mission of Sean Lasinker, CISO at Orica, to ensure those endpoints are always protected.

Founded in 1874, Orica has become one of the world’s leading mining and infrastructure solution providers. Operations range from the production and supply of explosives, blasting systems, mining chemicals and geotechnical monitoring to cutting-edge digital solutions and a range of services to sustainably mobilize the earth’s resources. The company employs over 13,000 engineers, scientists, technologists, operators, business specialists and on-site crew to support customers in surface and underground mines, quarry, construction and oil and gas operations.

Risk of Accidents

“The safety of our people, the communities we operate in, and our environment will always be our number one priority,“ shared Lasinker. “Ensuring our operational technology is used correctly, and we are prepared to respond to a cyberattack is of the utmost importance.”

Alongside the cybersecurity risk that all businesses face – like random phishing, ransomware, and unintentional employee mistakes – Orica has other security challenges. The company is at the forefront of research and development in new mining and blasting technologies and needs to ensure that the related data and information is safeguarded to protect the intellectual property.

Orica previously had an antivirus product in place, but it was complex to support, inefficient and a drain on resources. If there was a new risk detected, it had to be investigated and resolved manually. Endpoint protection and detection and response was basic and slow, offered limited threat-hunting capabilities and minimal visibility. When the product was acquired, Orica found support’s focus and attention lacking.

“The intention was always to aim for the next generation of endpoint security as part of our overall security strategy,” explained Lasinker. “We had come to the end of contract for our existing product and so it was the right time to find a modern, more efficient and effective solution.”

ORICA

INDUSTRY

Mining

LOCATION/HQ

Melbourne, Australia

CHALLENGES

- A cybersecurity breach could potentially affect safety
- Protecting intellectual property (IP) for innovative mining technology development
- Incident detection and response is consuming time and resources

SOLUTION

With endpoint protection as one of three key pillars of a security strategy, global mining services firm Orica is using CrowdStrike to protect worldwide staff and customers in remote locations who handle explosives and chemicals.

> “The standout feature of CrowdStrike — and what is making a difference to the business — is a single pane of glass visibility of endpoint security.”

Sean Lasinker
CISO
Orica

Orica researched and then ran a comparison between CrowdStrike and another next generation endpoint protection provider. The business decided to use CrowdStrike based on several criteria: These were ease of deployment, ongoing management, and the ability to integrate seamlessly with existing security and business systems such as a web secure gateway and an email security product. Besides the efficacy and functionality of the products, one of the key decision drivers was the clear roadmap and future scalability that CrowdStrike offered.

Protecting Remote Mining Locations

The IT environment that Orica needs to protect falls into three distinct technology pillars. First, Customer Systems that are sold to customers including digital solutions and internet of things (IoT) devices. Second, the Company's own Business Systems that are hosted on an AWS and Azure cloud infrastructure. Third, Manufacturing Systems, the Operational Technology (OT) that Orica uses to support several worldwide plants where, for example, explosives are manufactured.

Orica has deployed a series of products centered around CrowdStrike Falcon® Intelligence automated threat intelligence in all areas of its IT environment. This comprises 8,700 endpoints in Orica's global offices and manufacturing sites as well as engineers working in the field at customer mining sites.

Rollout was a joint effort between CrowdStrike and Orica, which Lasinker described as "seamless." The rollout consisted of CrowdStrike providing a detailed plan to migrate Orica from the legacy product to its own products. In addition to products, Orica also benefits from CrowdStrike services such as Falcon OverWatch which manages threat hunting.

The company recently signed up for the CrowdStrike Incident Response and Advisory Services Retainer, which enables Orica to prepare, in advance, to react quickly and effectively to a cybersecurity incident. It has proved invaluable in helping Orica assess potential threats and thwart them.

"Orica has already used the CrowdStrike Incident Response and Advisory Service twice to investigate a suspected security incident," said Lasinker. Thankfully in the two instances the incidents proved to be false positives. "Speed of response and resolution were pretty impressive but more importantly, it has given the business confidence and reassurance that if there are issues, it has the support and backup of CrowdStrike expertise and skills to help resolve them."

Orica is scaling up its CrowdStrike deployment with the rollout of solutions such as Falcon Device Control for USB security.

Lasinker asked his IT teams around the world what was noteworthy about CrowdStrike.

"The standout feature of CrowdStrike — and what is making a difference to the business — is a single pane of glass visibility of endpoint security."

"As a security expert and having that sort of information at my fingertips in real time — and being able to act at the click of a button — has saved a lot of time. The visibility we have compared to before is like night and day. With CrowdStrike — and the way it has been deployed across the business — we know we can rely on the accuracy and validity of the data."

RESULTS

Increases productivity and focus on value-add functions

Streamlines access to cybersecurity insurance

Improves endpoint security and builds business confidence

ENDPOINTS

8,700

CROWDSTRIKE PRODUCTS

- Falcon Device Control™ endpoint device control
- Falcon Device Control™ for cloud-delivered device control
- Falcon Insight™ endpoint detection and response
- Falcon OverWatch™ managed threat hunting
- Falcon Prevent™ next-generation antivirus
- Falcon Spotlight™ vulnerability management
- Falcon Intelligence automated threat intelligence
- Incident Response and Advisory Services Retainer

He added another standout feature is the ability to isolate multiple hosts at the same time. For example, Lasinker can highlight several endpoints that have specific indicators of compromise and act swiftly. "CrowdStrike enables us to quickly spot live incidents, gain greater visibility and discover unknown services, which is extremely efficient," explained Lasinker.

CrowdStrike proved critical in helping Orica deal with the 2021 Log4Shell threat with no impact. It was a software vulnerability within the popular Java logging framework, involving arbitrary code execution that affected multiple organizations around the world.

Saving Time, Money and Resources

Orica conducted a detailed analysis of the impact of CrowdStrike on the business and found that over a three-year period, CrowdStrike is expected to save over AS$1.5 million, pay for itself in 16.5 months and deliver a return on investment of 115%. With CrowdStrike's Real Time Response and remediation capabilities, the product has virtually eliminated the three weeks it used to take to recover and rebuild devices for remote workers. CrowdStrike has significantly reduced the burden on the small team that has to manage security 24/7 around the world, for example, cutting four hours to triage an incident down to 10 minutes. Time saved improves productivity and enables experienced staff to focus on more valuable activities.

Having CrowdStrike in the security portfolio also helps Orica manage cybersecurity insurance. Lasinker disclosed that cyber insurance premiums are rising across the industry as companies around the world face more cyber-attacks.

> "Having a best-in-class product such as CrowdStrike on our endpoints combined with the retained CrowdStrike Incident Response and Advisory Services goes a long way in providing reassurance of protections we have in place and our preparedness."

"As a CISO, there are three foundational aspects of cybersecurity we need to be good at and if we get them right, we have covered a significant portion of security risks. Number one is patching and vulnerability management, number two is regular backups and regular testing of those backups and number three is endpoint security. CrowdStrike handles the latter across the whole enterprise and as such is a critical security solution at Orica."

ABOUT CROWDSTRIKE

CrowdStrike, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

CrowdStrike: **We stop breaches.**