FIREEYE™

CUSTOMER STORY

Teck Resources

Securing Canada's Largest Metallurgical Resources Company

Teck

FACTS AT A GLANCE

INDUSTRY

Mining

SOLUTIONS

- FireEye Network Security
- FireEye Endpoint Security
- FireEye Managed Defense
- FireEye Threat Analytics
- FireEye Email Security
- FireEye Cloud MVX
- FireEye Central Management
- FireEye Helix

BENEFITS

- Integrated protection across multiple threat vectors
- 24/7 support from FireEye experts alleviates staffing challenges
- Ability to take a proactive stance with threat detection and remediation

CUSTOMER PROFILE

Teck Resources limited is the largest metallurgical resource company in Canada, focusing on the extraction of coal, copper, and zinc. As a global enterprise—with operating properties in North and South America, and interests around the world – the company's guiding values include safety, integrity, and respect; with a documented commitment to economic, social, and environmental sustainability.

While Teck Resources has earned its reputation as an innovator in the field of mining and metals, data is used as a key enabler across every aspect of the company's operations. Rob Labbé, director of information security, commented, "The disciplined application of data enables us to execute efficiently, manage costs and demonstrate to the communities in which we operate that we're working in a safe and environmentally friendly manner; all of which are critical to our company."

Data Keeps the Company Running

Data reliability is critical in enabling Teck to optimally administer its operations. "We turn data into a kind of kinetic motion that keeps our mines, plants, and smelters running," stated Labbé. "If we can't trust the information, everything comes to a grinding halt!"

He added, "If the integrity of our data is suspect we cannot operate our plants in the way they were designed to be used; and that has the potential to create a significant impact on operations."

One of the challenges of protecting an infrastructure that has the magnitude and complexity of Teck Resources' is the sheer volume of security-related data that is continually being produced. "We have a modestly-sized security team and sifting through the thousands of alerts that were being generated just to identify the handful of important notifications was becoming an insurmountable task," recalled Labbé. "We needed a better way of working."

> "FireEye gives us the capability to monitor network traffic generated by our control systems, providing us with the multi-vector protection and cross-enterprise visibility that is so critical."
>
> — **Rob Labbé,** Director of Information Security, Teck Resources

Fast, Accurate and Reliable

The Teck Resources team conducted an evaluation of potential approaches. "We elected to deploy FireEye Network Security because of its outstanding accuracy; when it does identify a threat, we have a high degree of confidence that it is real. On top of that, once detected, action is taken to immediately block the threat; this gives us the time to work on the root cause without having to simultaneously put out big fires like we used to," recounted Labbé.

Teck Resources opted to do a phased implementation; initially installing FireEye Network Security across its data center infrastructure, then out to field egress points, and finally to its global exploration sites.

Securing Even the Weakest Links

Having proved the effectiveness of the FireEye Network Security solution in the Teck environment, Labbé focused his attention on other potential vulnerabilities in the infrastructure. He elaborated, "The email threat vector can be a huge liability if not appropriately addressed. With the positive impact of the network security deployment, it was a logical choice to use FireEye Email Security."

Similarly, a need was identified to strengthen security across the company's massive number of endpoint devices. Labbé described, "As part of our due diligence we looked at a lot of options and while several were very proficient in certain individual areas, FireEye Endpoint Security delivers across the board and really excels at generating meaningful forensics information needed to investigate the root cause of an issue. This also ensures that I've got all the data from even before the attack occurred; I'm not trying to chase the shadow of what happened, I can see exactly what transpired."

Round-the-Clock Protection

The introduction of FireEye Threat Analytics is another key addition to Teck Resources' security stack. It elevates traditional SIEM technologies by applying threat intelligence, expert rules and advanced security data analytics to filter event data streams. "FireEye Threat Analytics enables my team members to further prioritize and optimize their response efforts. They're freed up from having to deal with background noise and are able to focus on the specialized tasks that really warrant their attention," affirmed Labbé.

To further enhance the effectiveness of his team, Teck Resources subscribes to FireEye Managed Defense. The service utilizes FireEye experts to provide round-the-clock monitoring of alerts from across the Teck infrastructure; they analyze alerts from the FireEye products deployed, network traffic recordings, security device logs and every endpoint in the environment. If a threat is detected, the Managed Defense team quickly pivots into investigative mode to collect evidence, create a timeline of events and construct a strategy that enables the Teck Resources security team to constrain risks and rapidly remediate the issue. The FireEye Managed Defense specialists act as an extension of the Teck team, providing expert advice to supplement in-house knowledge and to ensure that the environment stays secure. They also proactively hunt for non-malware based threats such as credential misuse and for other indicators of threat activity.

"Managed Defense helps us to not only cover our off-hour periods but also cope with inevitable surges in workload. Because the rate of alerts is highly volatile – and very unpredictable – it's unrealistic to staff for the spikes: Managed Defense enables us to smooth out the peaks and troughs. Now, when we receive an alert we let FireEye Managed Defense triage and perform the initial assessment to determine the severity of the threat. My team can then proceed with the intelligence needed to perform a definitive investigation," Labbé observed. "Managed Defense enables us to provide uninterrupted industrial-strength coverage, and completely streamlines how we respond to and remediate issues."

Simplifying Security Operations

Also woven into the FireEye cross-enterprise threat prevention fabric is FireEye Helix. An operations platform that expands visibility, accelerates response, and lowers security cost, Helix streamlines security processes. "Helix really is bringing the FireEye stack of products and services into a single platform," said Labbé, "The openness of Helix allows us to use FireEye as our core and easily integrate third-party vendors when we need them."

Helix works as a seamless and scalable foundation to connect and enhance security solutions within Teck Resources. Empowering the security team to efficiently conduct primary functions, FireEye Helix surfaces unseen threats and accelerates response times. Automated work

> “FireEye Threat Analytics enables my team members to further prioritize and optimize their response efforts. They’re freed up from having to deal with background noise and are able to focus on the specialized tasks that really warrant their attention.”
>
> — **Rob Labbé,** Director of Information Security, Teck Resources

flows coalesce related data to help drive faster decisions and minimize the impact of a security breach. “Orchestration and automation is already configured within Helix, so there is no need to spend time or dedicate resources to replicate those functions. Helix streamlines our security so we can spend its time solving security problems.”

IT or OT – It Doesn’t Matter to a Cyber Criminal

The complexity of the Teck Resources environment extends beyond the traditional information technology landscape. “We rely on a significant operational technology [OT] infrastructure to control and monitor our production systems,” explained Labbé. “Because OT components also are vulnerable to malicious threats, we’re deploying FireEye technology into plants and mines. In addition to coverage of our IT domain, FireEye gives us the capability to monitor network traffic generated by our control systems; providing us with the multi-vector protection and cross-enterprise visibility that is so critical.”

Out of Sight but Not Out of Mind

FireEye Cloud MVX provides a public cloud deployment of the renowned FireEye MVX engine, providing organizations with the ability to deliver real-time detection and blocking of threats anywhere across the infrastructure.

With many operations located in distant and sometimes very remote locations, ensuring that each site is equipped with the latest threat intelligence was a major challenge for Labbé. He explained, “Prior to subscribing to the Cloud MVX service, the huge disparity in the quality of connectivity we have across our locations—including facilities in Namibia and the Gobi Desert—created potential for exposure. We’re now assured that we have the latest intelligence in place. We also can take advantage of new capabilities and functionality as soon as they are released, without suffering delays caused by poor network connections with one of our primary hubs.”

He continued, “And if for whatever reason the cloud is inaccessible at a particular site, then there’s no external network traffic to worry about anyway. For me FireEye Cloud MVX is a no-brainer!”

Staying Ahead

Labbé reflected, “Security solutions have to constantly deliver the necessary protection but remain flexible enough to adapt to business changes. In hockey terms, good players don’t chase the puck around the ice, they anticipate where it’s going to be and are waiting for it when it gets there. It’s really the same thing with security and that’s what FireEye is helping us to do.”

He concluded, “My analysts used to be constantly reacting to alerts which—for people with the deep knowledge of the company and the business they possess—is definitely not the best use of their skills. With the FireEye solutions and services, my team now can dedicate time to the proactive and preventative security measures that enable Teck Resources to deliver on our environmental, economic, safety and social commitments.”

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

FIREEYE™