

Mining and Metals Giant Protects Its Operational and Reputational Integrity

The company reduces exposure to financial or brand harm with risk-based vulnerability management enabled by Kenna Security

Understanding the Operational and Reputational Risk

When you think of the mining industry, you might envision huge mountaintop operations, shattering dynamite blasts, and giant vehicles hauling away a precious commodity. And you'd be right. But contrary to the heavy-industry feel of this image, modern mining is as much a digital business as it is a physical one. Case in point: a leading international mining company and one of the world's largest copper producers.

With major mining operations throughout the world, the company must be efficient to compete effectively. And it is: the company is renowned across the industry for its operational efficiency. The company uses advanced digital systems for blast management, mine operations, lightning detection, environmental data collection, and even predictive analytics based on equipment sensors to ensure life safety and plan maintenance windows. These systems enable the company to keep its employees safe while helping the business generate strong financial returns, a large portion of which the company invests back into the communities where it operates in the form of vital infrastructure like communications systems, schools, hospitals, and water and sewer systems.

The data-driven operational, health and safety, and environmental systems are fundamental to the company's financial and reputational well-being. The Global Manager Security Governance and Communications points out, "If a hactivist got into our systems to manipulate data in some way, they could disrupt operations or cause great reputational harm. It could cost the company millions per day, and even put at risk our license to operate in that particular region."



Lowering our risk scores means we've reduced the potential exposure of the business for someone to compromise our operations or reputation. Since we're a publicly traded company, we have to think about the impact that mine downtime or bad press has on stockholder confidence. Ultimately, lower risk puts us in a stronger position to build profitability and value as a company."

Global Manager-Security Governance and Communications

Customer: Global Fortune 500 mining company

Industry: Mining and metals

CHALLENGE:

Gain greater control over vulnerabilities to protect operational and reputational integrity

SOLUTION:

Kenna.VM to align vulnerability remediation with business priorities based on risk

RESULTS:

- Lowered overall risk score for critical systems by nearly 80%; total assets by about 50%
- Greatly reduced the risk of vulnerabilities across thousands of geographically dispersed assets
- Positioned the company to build greater profitability and value for stockholders by reducing risk exposure
- Enabled IT executives to make informed decisions on where to focus remediation efforts
- Accelerated maturity of vulnerability management program with easy-to-use risk analysis
- Helped staff improve focus of vulnerability remediation to maximize efficiency and effectiveness



Measuring Risk, Not Just Vulnerabilities

The Global Manager-Security Governance and Communications faced a dormant vulnerability management program when joining the organization. There had been some attempts at raising risk awareness and implementing security measures, but nothing had gained traction. “As the person in charge of global information risk, one of my prime objectives was to rectify our vulnerability management,” the global manager said. “We started by implementing a new scanner and taking an inventory of what assets were actually out there. Then we looked at addressing the vulnerabilities at a very high level—what’s critical, what’s high—but it was all count-based.”

As the vulnerability management program advanced, the company wanted to gain a better perspective of vulnerabilities based on actual risk to the company, not just how many there were. A corporate risk assessment was performed to identify which IT resources (systems, data sets, applications, etc.) were essential for generating revenue and ensuring employee safety, to determine which assets should have their vulnerabilities remediated first. Even with that, they wanted a way to measure the specific level of risk posed by each vulnerability.

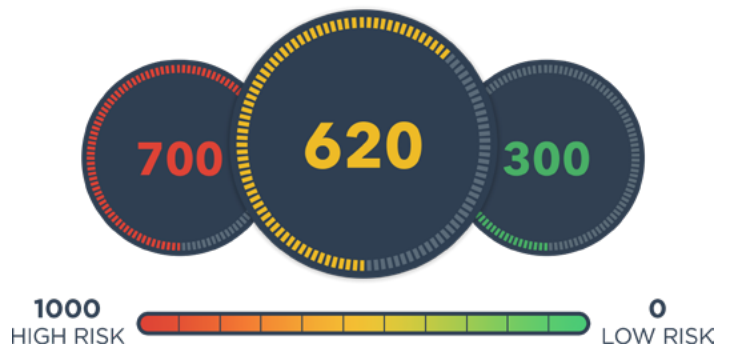
“I wanted a tool like Kenna to help us identify those risks, to see what’s happening in the wild versus what we think is out there. We needed a tool that would help us prioritize vulnerabilities in a way that didn’t just point us to which systems were critical, but which ones posed the greatest risk to the financial and reputational integrity of the company,” said the Global Manager.

The company evaluated several potential solutions, ultimately concluding that Kenna Security’s vulnerability management solution, Kenna.VM was the right decision. “With Kenna, we have

ability to isolate particular systems into groups of risk meters, which allows me to determine at a higher level where our most critical risks are, and where we should focus our vulnerability management efforts. We can categorize those truly critical assets and apply a credible risk score to them based on real-time exploit intelligence.” said the Global Manager.

Aligns Remediation Effort With Business Priorities

In rolling out Kenna.VM, the security team imported data from their existing vulnerability scanner, Tenable, into Kenna.VM. Kenna combines global intelligence data, billions of managed vulnerabilities, global attack telemetry, and remediation intelligence to accurately track and measure real-world exploit activity across the enterprise. Kenna.VM then analyzes these data sources to deliver an accurate, quantifiable risk score for every vulnerability and asset. The company was now able to gain the context it needed to take a risk-based approach to vulnerability management, effectively prioritizing which vulnerabilities need to be remediated first.



Or, as the Global Manager said: “Kenna provides an easy way to prioritize vulnerabilities and put them into a business perspective so management can make decisions on which vulnerabilities to focus the IT teams on. This fostered acceptance of Kenna across the organization and really helped us gain traction with our vulnerability management program.”

He adds that having a risk-based approach from Kenna not only aligns vulnerability remediation with business priorities, but also avoids wasted effort addressing issues that pose little to no risk. It provides validated evidence of the business risk so security, IT, and management have context for the broader impact of the vulnerability.

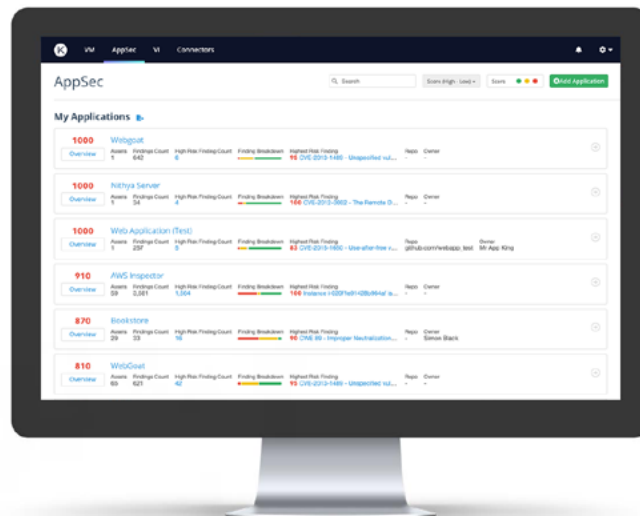
One example is the vulnerability POODLE.

“Fixing POODLE in our internal applications may not be a high priority, but the assessment may be very different for our external-facing applications when you look at it from a risk-based perspective,” said the Global Manager. “That’s something we can see easily in Kenna, whereas in a tool like Tenable, assets in both environments would be displayed with the same threat level.”

To further illustrate the point, the Global Manager said: “Our CIO has said to me, ‘the reason IT and security executives get fired is because they didn’t take care of things they knew about. Without knowing the true risk of a vulnerability, I won’t have enough context to assign it the appropriate priority level. That could lead to a breach, which is bad for everyone. On a monthly basis I present my Kenna Risk Scores and all the associated trending data to our CIO. This allows him to make decisions for his organization on where to focus the efforts of his team to manage risk. It’s targeted and strategic, as opposed to saying here are 200,000 vulnerabilities, go fix them all.”

Lower Risk Score Positions Business To Build Profitability

Leveraging the intelligence of Kenna.VM to focus on reducing overall risk, not just reducing the number of vulnerabilities, has had a profound impact on the business. Within seven months of deploying Kenna, the company lowered its risk score for all assets by just under 50 percent, and for critical systems, such as SAP and associated applications, by nearly 80 percent.



“Lowering our risk scores means we’ve reduced the potential exposure for someone to compromise our operations or reputation. Since we’re a publicly traded company, we have to think about the impact that mine downtime or bad press has on stockholder confidence. Ultimately, lower risk puts us in a stronger position to build profitability and value as a company.”

Seeing the impact of Kenna.VM on reducing risk across corporate assets, the company is now looking at extending his risk-based vulnerability management capabilities to DevOps teams by adding Kenna’s application security solution, Kenna.AppSec.

“Like lots of businesses we have auditors come in and present us with a long list of application vulnerabilities that need to be fixed,” said the Global Manager. “We need to be able to focus in on those vulnerabilities from a risk perspective, and we see Kenna.AppSec as a smart way to do that.”

The Global Manager concludes, “A solution like Kenna.VM is truly needed today due to the sheer number of vulnerabilities out there, and all the new ones coming tomorrow. You’re never going to get them all, so you better focus remediation efforts on the vulnerabilities that present the greatest risk to the business. For us, the key has been our ability to provide risk-based insights to our executive leadership so they are better informed when making those decisions.”

To learn more about aligning your organization around risk visit www.kennasecurity.com

KENNA
Security