CASE STUDY

Global leader in metals mining & manufacturing enhances network visibility & access control with Portnox CORE

ArcelorMittal

Executive Summary

JSC ArcelorMittal Temirtau (AMT) is one of the world's largest integrated mining and metallurgical complex, with its own coal, iron ore and energy base.

AMT is a part of ArcelorMittal, a global leader in metals mining and manufacturing. The company boasts a workforce of more than 200,000 across 60 countries, and an annual production capacity of approximately 118 million tonnes of crude steel.

Earlier this year, Alexandr Chsherbov, the group's principal security engineer, together with his team, performed an in-depth security analysis and concluded that they required better visibility of the devices and components connected to the company's network.

Furthermore, Chsherbov wanted the ability to control which devices could gain access to the network in accordance with the company policies, security regulations and general network best practices.

To help achieve these goals, the company turned to Portnox CORE to successfully secure their networks and automate security processes.

INDUSTRY:
Mining & Metallurgy

SOLUTION IMPLEMENTED:
Portnox CORE

BENEFITS:

Rapid Deployment – CORE is agentless, centralized and works with any existing equipment and vendors.

Simple Operations – CORE's operational console provides a unique network-focused view (from bare metal to endpoint) as well as endpoint listings and the ability to filter the information easily.

Scanning & Patching Automation – Processes that were otherwise labor-intensive.

Compliance Checks – With improved visibility of devices and levels of access, AMT can ensure network compliance across its entire organization - no matter where employees are located.

The Challenge

ArcelorMittal Temirtau was faced with a challenge common amongst large manufacturers: a general lack of visibility across their networks, and in turn increased vulnerability to security and compliance issues.

"We were blind. We couldn't control the devices that were connected to our network or be sure that the devices that were connected were compliant with company policies. If they were non-compliant, there was nothing we could do about it," said ArcelorMittal Temirtau CIO, Nestor Komarnitskiy.

"We have large sites across Kazakhstan and we needed the ability to secure user access to our wired switch ports as well as to our APs," Komarnitskiy continued.

Why Portnox CORE?

The information security team at AMT needed a solution that could be easily deployed and maintained, while providing full visibility and enforcement capabilities. After testing some of the most well-known NAC solutions on the market, the group decided to implement Portnox CORE. “We decided to go with Portnox CORE because it was easy to deploy, affordable, agentless, offered a simple licensing model, and required minimal investment in new infrastructure,” said Alexandr Chsherbov.

> *At AMT we needed to find a fully comprehensive NAC solution that didn’t add complexities in terms of excessive additional hardware, agent installation and additional infrastructure investment. We examined a few products, and after testing, we couldn’t be happier with the ease of deployment and on-going management of Portnox CORE. We were able to discover devices we didn’t know about and took strides to either remove them from the network or approve them via the Portnox platform.*
>
> ***Nestor Komaarnitskiy, CIO @ ArcelorMittal Temirtau***

The Impact

CORE rapidly provided a complete, real-time view of the network and every device that was connected or trying to connect to it. This included identifying and categorizing all devices, including company-issued computers as well as smartphones, tablets and IoT devices – all without having to install an agent.

As access is based on user identities, both company devices and contractors were quickly accounted for, including their location and the area of the network they had access to. With access to information such as endpoint type, operating system, configuration, software and applications, patch state and more, Chsherbov’s team was able to take action on new insights. “We can now rest assured that rogue devices can’t connect to our network. Plus, our IT support capabilities have drastically improved – it’s easy for our support technicians to find users and their devices via the NAS view,” said Chsherbov.

With Portnox CORE fully implemented, AMT’s security team has been able to handle all challenges associated with device visibility, access control and network compliance enforcement. The organization can now see all endpoints on the network and ensure that they are properly secured and patched according to company policies, privacy standards and regulatory compliance. As risk monitoring and enforcement actions are automated, AMT’s IT team has been able to devote more time to other important tasks that would otherwise have to be done manually, and thereby increase efficiency and productivity.