# Global Mining Company Case Study

Securing IoT Devices with Cisco Secure Workload

## About the Customer

A global leader in metal materials and process solutions for aerospace, transportation, defense, energy, and industry.

## Business Challenges

The customer operates their business with many **Internet of Things (IoT) devices**. These controllers, sensors, and other components provide **essential management and operations** of customer foundries and fabrication systems. They are also IP connected to the corporate network and require appropriate security controls (e.g. segmentation) as an essential component of an effective security architecture. The technology team had planned to use firewalls for workload protection, but without full knowledge of traffic flows, it was unclear which rules to put in the firewalls.

## Solution

BTA deployed Cisco Secure Workload (CSW, formerly Tetration) to monitor traffic and determine what flows should be permitted. Since the IoT devices run limited, special-purpose operating systems, the typical data collection method (via CSW software agent) could not be utilized. BTA deployed Encapsulated Remote Switched Port Analyzer (ERSPAN) collectors to import full flow (unsampled) information into CSW to capture and analyze all traffic over our typical four-to-five-week data collection period.

The BTA team took this data to build traffic policies in CSW based on the groupings the customer defined by manufacturing processes, business organization, and network objects. The unsampled flow information collected by Cisco Secure Workload was essential for defining complete and accurate security policies.

Using CSW, BTA was able to build deterministic permit-and-deny policy. Leveraging CSW's automation capabilities, BTA provided **comprehensive, human-readable policy reports.** These policy reports clearly indicated which devices should be communicating, over which protocols, to deliver the customer's business requirements. The reports covered IoT and non-IoT components across the customer's infrastructure, providing an end-to-end security blueprint. The customer team was able to quickly and confidently map those policies to their firewall rules, securely segmenting their traffic **without the risk of disrupting their complex manufacturing processes.**

## Business Outcomes

At BTA, we are very deliberate about our processes. We executed step-by-step, using our proven, **repeatable S.I.M.P.L.E. service delivery process,** to ensure that we focus on exactly what was necessary while eliminating the "noise" - saving the customer time and resources.

The ultimate business outcome for the customer was the deployment of effective network security segmentation for:

- Dozens of applications
- Over Hundreds of IP devices
- Across 20 separate manufacturing processes (each of which represents an entire supply chain of steel production)
- All without incident or downtime.

## About BTA

BTA simplifies complex technology implementation. As a Cisco Digital System Integrator (DSI) Partner, they've helped 500+ North American enterprises transition to SDN with Cisco ACI.

**Schedule A Call**

info@gobta.com 678-951-8980 gobta.com