BUSINESS TECHNOLOGY ARCHITECTS

CASE STUDY

GLOBAL MINING COMPANY

Securing IoT Devices with BTA's Policy Automation Engine (PAE)

BTA's Policy Automation Engine (PAE) combines device intelligence and field-proven processes to enable quick & secure application segmentation, at multiple policy enforcement points.

ABOUT THE CUSTOMER

The customer is a global leader in metal materials and process solutions for applications in the aerospace, transportation, defense, energy, and industrial spaces.

BUSINESS CHALLENGE

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.

.

CISCO and BTA's 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. Using CSW, the BTA team took this data and built traffic policies in CSW using groupings that the customer defined according to their manufacturing processes, business organization, and network objects. The unsampled flow information collected by CSW was essential to defining complete and accurate security policies.

BTA's Policy Automation Engine (PAE) was deployed to provide comprehensive, human-readable policy reports from the CSW-defined policies. The PAE reports connected host-based rules to site-based firewalls. These policy reports clearly indicated which devices should be communicating, over which protocols, to deliver the customer's business requirements. The PAE reports covered IoT and non-IoT components across the customer's infrastructure, defined in the language of the business, 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 OUTCOME

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 without incident or downtime for:

- Dozens of applications
- Hundreds of IP devices
- 20 separate manufacturing processes, each of which represents an entire supply chain of steel production