Originally acquired for OT security, a global manufacturer discovers the operational benefits of Microsoft Defender for IoT

With over $5 billion in annual revenues, this global public manufacturer operates sites in more than 25 companies. In 2018, they recognized that their lack of visibility into ICS/OT asset inventory was a liability and it hindered their ability to manage the risks associated these assets.

This stood in sharp contrast to their advanced IT security maturity, which included Endpoint Protection Platforms (EPP), Endpoint Detection and Response (EDR), Vulnerability Management (VM), Cloud App Security Broker (CASB), security information and event management (SIEM) system, firewalls, network access control, and an IT ticketing system just to name a few. When searching for an OT security platform, it was important that the solution would seamlessly integrate with an existing IT security stack which included solutions from a variety of different vendors. The company also planned to centralize OT and IT security and needed to demonstrate a safety- and security-first environment to auditors.

When Microsoft Defender for IoT was deployed in their first plant, the company was impressed with how quickly they were able to discover their complete asset inventory. Once the sensor was deployed asset inventory was discovered within minutes. Their larger concern, however, was to determine if there were any existing IT/OT security threats and vulnerabilities in their network. With the click of a button, the team generated a Risk Assessment report and then leveraged it to prioritize mitigations. In the report they were able to identify unauthorized devices running on the network, at-risk devices that are connecting to the internet, high priority security patches for devices where patching is a viable option and finally the top attack vectors that attackers would exploit if given the chance. These are just a few examples.
Providing value, right out of the gate

The deployment of Microsoft Defender for IoT in the first seven plants went more quickly than originally scheduled and it began providing what this long-time member of the Fortune 500 list described as “immediate value.” When a recently upgraded laptop started flooding its local network with scans, leading to a disruption in PLC communications and intermittent downtime, the team searched in vain for the source of the problem.

After 36 hours without success, the CISO suggested checking Microsoft Defender for IoT. Within five minutes, the laptop in question was located and the problem was resolved. In the meantime, however, halted production caused more than $1 million in top line losses at this 24/7 facility. Microsoft Defender for IoT is now their first stop when a root-cause analysis of an operational issue is needed.

Had the downtime gone on longer, they could have lost additional millions due to a single employee’s networked laptop with a misconfigured RSLogix application. While the board and CISO were originally searching for a platform to deploy quickly, discover assets, manage risk and vulnerabilities, provide threat monitoring and integrate with their existing IT stack, they discovered that Microsoft Defender for IoT can also provide valuable assistance when diagnosing and resolving operational equipment issues as well.

For more insights on how Microsoft Defender for IoT benefits the manufacturing industry, visit the manufacturing landing page today.